

**ANNEX V to the
Memorandum of Agreement between the
Transportation Security Administration and the
Federal Aviation Administration**

INTELLIGENCE

1. Purpose. The Transportation Security Administration (TSA) and the Federal Aviation Administration (FAA) ("the Parties") have a mutual interest in ensuring security and safety in aviation. To achieve this purpose, the Parties agree to abide by the terms of this Annex, subject to applicable federal laws, regulations, and policies.

Under the Aviation and Transportation Security Act (ATSA), P.L. 107-71, 115 Stat. 597, in addition to various other statutory mandates, the Under Secretary of Transportation for Security is responsible for receiving, assessing, and distributing intelligence information related to transportation security and serving as the primary liaison for transportation security to the intelligence and law enforcement communities. 49 U.S.C. § 114 (f)(1) and (5). As a result of ATSA, the Transportation Security Intelligence Service (TSI), an office within TSA, subsumed the bulk of the former FAA Office of Civil Aviation Security Intelligence (ACI).

Because TSI's intelligence functions support FAA's mission and are necessary to the operations of certain FAA programs, TSI will continue to provide intelligence support to FAA pursuant to this Annex. Any information/intelligence provided by TSA to FAA under this Annex shall also be provided, as soon as possible, to the Secretary of Transportation's Director of Intelligence and Security, S-60.

2. Definitions. As used in this Annex:

a. The term "coordinate" means to take action which provides reasonable notice of an agency's activities and which affords the notified agency, when possible, a reasonable opportunity to address concerns raised by such notice.

b. The term "intelligence" in most contexts herein means national security information (that is, information that is classified in accordance with E.O. 12958) generated by producer agencies of the U.S. Intelligence Community.

c. The term "reasonable notice" means as soon as possible, preferably prior to action, without placing an activity in jeopardy.

3. Responsibilities.

a. General Coordination. The Parties shall make continuing good-faith efforts to coordinate on (i) addressing the missions and interests of the other Party, (ii)

avoiding duplication or conflict in agency authorities, (iii) providing consistent and authoritative information to the U.S. Congress, stakeholders or other interested parties, and other persons, and (iv) furthering the transportation security interests of the United States. The above-described efforts to coordinate shall commence as soon as reasonably practicable under the circumstances, preferably at the earliest stage of development.

b. Sensitive Security Information. The Parties will take actions necessary to protect Sensitive Security Information (SSI) designated such by FAA pursuant to former 14 CFR Part 191, by TSA pursuant to 49 U.S.C. §114(s) and 49 CFR 1520, or by DOT pursuant to 49 U.S.C. § 40119.

c. Intelligence Requirements. The Parties agree that each has the following intelligence responsibilities:

(1) The Office of Security and Investigations (FAA/ASI) is the point of contact within FAA for all intelligence requests. All FAA Lines of Business (LOB) will provide draft Statements of Intelligence Interest (SII) to FAA/ASI which will vet and consolidate such requests, review arrangements for receipt, handling and storage of classified intelligence information by the respective LOB and forward validated requirements to TSI. FAA/ASI will provide TSI with a consolidated SII that reflects the need for intelligence information for all FAA LOBs.

(2) TSI will forward FAA's consolidated SII along with TSI intelligence requirements to the Intelligence Community (IC) and federal law enforcement agencies that produce intelligence information.

(3) TSI will share with FAA intelligence and law enforcement information TSI receives. TSI will also share with FAA, TSI's own analysis that is responsive to FAA's SII. TSI will make this information available to the concerned FAA LOB, FAA/ASI, or other designated Point of Contact, consistent with security requirements.

(4) As appropriate TSI will draft and propose to IC producers lower classification or unclassified releases of information in support of FAA operational requirements.

d. General TSI support to FAA. TSI will continue to provide a daily news service to select FAA recipients and continue to produce and disseminate the Transportation and Aviation Security Intelligence Summary (TASIS) on a weekly basis to FAA/ASI field elements. Additionally, TSI will continue to provide ad hoc intelligence briefings to senior FAA officials.

e. Special Security Office Support. TSI will continue to provide special security office support.

(1) TSI will maintain and pass Sensitive Compartmented Information (SCI) clearances for FAA and indoctrinate for certain special access programs as required, and will coordinate special security clearance matters with IC entities on the behalf of FAA.

(2) TSI will receive, make available, and control SCI information in support of FAA national programs.

(3) FAA will provide TSI with all security clearance information needed to process FAA SCI access eligibility determinations and will provide TSI with an accurate security clearance roster the first business day of every month.

(4) FAA is responsible for the investigation, adjudication of investigative results, and granting of security clearances for FAA personnel and for the determination of the need-to-know SCI for FAA personnel being nominated for SCI access.

f. Indications and Warning. TSI will continue to provide to FAA 24 hour/7 day a week threat indications and warning support.

g. TSI Support of the FAA Assistant Administrator for Information Services and Chief Information Officer (FAA/AIO) and other FAA Elements With Respect to Cyberthreat and Cyberattack Matters. The Parties will support each other in the following manner:

(1) In monitoring and analyzing the nation-state, terrorist, and hacktivist cyber threats, TSI will provide any such information as appropriate to FAA.

(2) TSI will provide FAA/AIO intelligence information on hacker and other attack tools, methodologies, and intentions, to include obtaining sanitized versions of intelligence information as required.

(3) FAA/AIO will notify FAA/ASI and TSI of root level intrusions, web page defacements, and other incidents involving data systems.

(4) FAA/AIO will be responsible for analysis and action with respect to technical vulnerabilities and net risk to FAA cyber systems but will defer to TSI the receipt and analysis of threat information regarding the nation-state, terrorist, and hacktivist cyber threats.

(5) FAA/AIO will continue to provide FAA liaison at the National Infrastructure Protection Center (NIPC) and operational data systems security contacts with certain elements of the National Security Agency but will insure that all raw and finished intelligence received from such entities is fully coordinated with TSI and the designated ASI point of contact, and validated.

(6) With respect to any FAA data systems not under the cognizance of FAA/AIO, TSI will provide the same type and level of support as that described in subparagraphs (1) through (5) above to the FAA LOB responsible for the system in question. FAA/ASI will coordinate the requirements for TSI support of such requirements to prevent unnecessary duplication of effort by TSI.

h. International Aviation and Crisis Response Working Group Support. TSI will support FAA International Aviation and Crisis Response Working Group in the following manner:

(1) TSI will monitor and report to FAA information on military or paramilitary situations abroad in which military or paramilitary capabilities could pose a threat or risk to U.S. civil aviation safety, and on the hostile use of or threat to use stand-off weapons against U.S. civil aviation.

(2) TSI will assist FAA in coordinating proposed sanitized releases of information with intelligence and law enforcement elements (such as the Departments of Defense and State) for inclusion in Notices to Airmen (NOTAMs), Special Federal Aviation Regulations and other regulatory or administrative actions.

i. Threats to the Global Positioning System (GPS), Related Systems and Critical Air Navigation Systems.

(1) TSI will support the FAA Office of Communications, Navigation and Surveillance (CNS) (FAA/AND) and Airway Facilities Service (FAA/AAF) concerning potential and current threats to the National Airspace System including CNS Systems under development, including augmentations to the Global Positioning System (GPS) currently called the Wide Area Augmentation System (WAAS) and the Local Area Augmentation System (LAAS).

(2) TSI will also provide threat indications and warning and information to concerned FAA elements concerning the potential use of radio frequency or directed energy weapons to disrupt civil aviation or of any other threats to radars, communications systems or ground based navigational facilities.

(3) FAA elements will inform TSI of any significant disruption of an unknown or possibly hostile nature to the WAAS, LAAS or other critical air navigation systems.

j. FAA Associate Administrator for Regulations and Certification. TSI will support FAA Associate Administrator for Regulations and Certification (FAA/AVR) in the following manner:

(1) TSI will support FAA/AVR and subordinate entities by providing information concerning threats involving areas for which FAA/AVR is responsible (such as General Aviation, flight schools, airman certification, airworthiness, and matters

involving several elements of FAA, such as stand-off attacks, including Man-Portable Air Defense System (MANPADS)).

(2) FAA will assist TSI in the dissemination of threat information.

k. FAA Associate Administrator for Air Traffic Services. TSI will support FAA Associate Administrator for Air Traffic Services (FAA/ATS) in the following manner:

(1) TSI will support FAA/ATS and subordinate entities by providing information concerning threats involving all areas for which FAA/ATS is responsible, including for example, but not limited to: hijacking, threats to aircraft from stand-off weapons such as Man-Portable Air Defense Systems (MANPADS), sabotage of systems, attacks upon facilities and personnel under ATS control and interference with air-ground communications.

(2) The Parties will work together in the crafting of suitable language concerning threats when such is needed for use in Air Traffic Bulletins, and other communications from the Administrator to air traffic controllers or to support Air Traffic actions in support of security objectives pursuant to Annex XI to this MOA.

(3) TSA will provide all forms of threat indications and warning, to include cyber threat, pursuant to subparagraph g.(6) above, to the ATS subordinate element responsible for security of the NAS.

l. TSI support of Other FAA Elements Responsible for the Security of Facilities, Personnel or Operations. TSI will support FAA/AAF, FAA/ASI and other FAA elements concerned with, or responsible for the security of FAA facilities and personnel.

(1) TSI will provide intelligence support, coordinated through FAA/ASI for FAA Administrator and all LOBs and staff offices, with respect to actions to protect FAA personnel, facilities, resources, and operations.

(2) The Parties will work together in validating the threat information concerned and in crafting suitable language concerning threats when such is needed for use in General Notices (GENOTs) and other communications from the Administrator to FAA facilities, managers and personnel.

m. FAA Associate Administrator for Commercial Space Transportation (FAA/AST). The Parties will support each other in the following manner:

(1) FAA/AST will provide TSA/TSI information on commercial space transportation activities so that TSI can better support FAA/AST. This information will include both a basic overview of commercial space transportation activities and specific

advance notice of upcoming commercial launch and reentry activities, consistent with notifications also delivered to U.S. Space Command.

(2) TSI will provide FAA/AST threat indications and warning support.

n. FAA Sensitive Activities Program. TSI and FAA Sensitive Activities Program (SAP) will work together in the following manner:

(1) Until such time as FAA elects to move SAP elsewhere or TSI relocates out of Sensitive Compartment Information Facility (SCIF) space in FOB 10A, both Parties agree that SAP will be provided office space within FAA-provided, TSI-operated SCIF.

(2) Consistent with security standards for classified systems, TSI classified data and communications systems will continue to be used to support SAP as long as TSI remains in FOB 10A.

(3) TSI Liaison officers at IC agencies and the FBI, and TSA-funded personnel on the El Paso Intelligence Center (EPIC) Air Watch, will continue to facilitate the coordination of FAA Sensitive Activities matters until such time as FAA establishes direct coordination with the agencies concerned.

(4) FAA agrees that any SAP matters that involve passenger-screening, access to airport secure areas, or other matters of TSA interest will be promptly coordinated with TSA.

o. The El Paso Intelligence Center. FAA will retain its Program Manager at EPIC and control of all FAA-supplied equipment and data. FAA will provide technical assistance and maintenance support, on a reimbursable basis to EPIC, to maintain FAA-supplied data systems in accord with separate understandings between FAA and EPIC. TSA personnel will continue to access and use FAA-supplied data in accord with protocols between FAA and EPIC.

p. FAA support of TSI. In addition to the other responsibilities of FAA detailed in other portions of this Annex, FAA will support TSI in the following manner:

(1) FAA will continue to provide suitable office space. TSA is responsible for all security matters dealing with this space. This includes current TSI SCIF spaces and additional contiguous space on the third floor of FOB 10A.

(2) FAA will continue to provide utilities, local telephone, data circuits, access to existing FAA databases such as the Airman/Aircraft registry, and special telecommunications support. In addition, FAA will continue to provide TSI custodial service, motor pool access, mail room services, health clinic services, publication support, parking in the A-Level garage for shift workers and as-needed crisis

management response by day workers, and other common services on the same basis as such are provided for FAA elements in building FOB 10A.

q. Actions that Require Departmental Approval. In addition to the coordination described above, if either Party engages in activities which could ultimately result in an action requiring the approval of the head of the Department in which either Party operates, the Parties will follow any applicable Departmental approval and coordination policies.

4. Funding and Resources.

a. No funds will be transferred pursuant to this Annex. Any changes to the services provided by either Party will be subject to a separate agreement that will address resources.

b. As long as TSA/TSI continues to provide the intelligence support of FAA, FAA agrees not to seek the transfer of personnel and other assets being used by TSI to support FAA to FAA control.

5. Termination. In view of the relatively long lead times required to acquire and accredit Sensitive Compartmented Information Facilities (SCIFs) and communications systems and to recruit, train, obtain, and clear new staff, both Parties acknowledge the need to provide as much lead time as possible for proposed major changes in the arrangements set forth in this Annex; acknowledge that renegotiation of the terms of this Annex and the division of resources concerned would be required; and agree to work cooperatively to ease any transition of intelligence or logistical support. Accordingly, the Parties agree to provide written notice of any Party's intention to terminate this Annex.

6. Points of Contact. For purposes of initiating coordination required by this Annex, the point of contact in the agency taking action, or the point of contact's designee, shall communicate with the point of contact of the affected mode, or the point of contact's designee. Subject to updates by the Parties, the following shall constitute points of contact with respect to this Annex:

TSA:

Assistant Administrator for Intelligence
Transportation Security Administration
800 Independence Avenue, S. W. Suite 317
Washington, DC 20591

FAA:

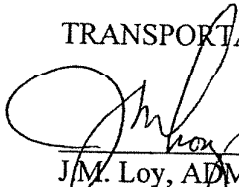
Manager, National Security Coordination Staff
Office of Security and Investigations
Federal Aviation Administration
800 Independence Avenue, S.W., Room 308b
Washington, DC 20591

S-60:

Assistant Director For Intelligence
Office of Intelligence and Security
Department of Transportation
400 Seventh Street, S.W.
Washington, DC 20590

APPROVED BY:

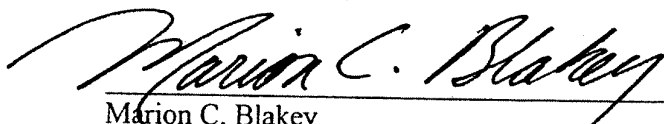
TRANSPORTATION SECURITY ADMINISTRATION



J.M. Loy, ADM
Under Secretary of Transportation for Security

2/28/03
Date

FEDERAL AVIATION ADMINISTRATION



Marion C. Blakey
Administrator

2/28/03
Date